The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE ISSUED:

08/13/2014

SUBJECT:

Multiple Vulnerabilities in Google Chrome Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Google Chrome that could result in remote code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the user running the affected application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

At this time, there is no known proof-of-concept code available.

SYSTEMS AFFECTED:

- Google Chrome Prior to 36.0.1985.143

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium government entities: **High**
- Small government entities: **High**

Home users: High

TECHNICAL SUMMARY:

Twelve unspecified vulnerabilities were patched in the latest version of Google Chrome. The only three that were mentioned specifically were as follows:

- A use-after-free vulnerability that existed in web sockets. [CVE-2014-3165]
- An information disclosure vulnerability due to an error in SPDY. Attackers can exploit this issue to obtain sensitive information. [CVE-2014-3166]
- Various fixes from internal audits, fuzzing, and other initiatives. [CVE-2014-3167]

These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation could result in an attacker gaining the same privileges as the user running the affected application. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable Google Chrome products immediately after appropriate testing by following the steps outlined by Google.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or un-trusted sources.

REFERENCES:

Google:

http://googlechromereleases.blogspot.com/2014/08/stable-channel-update.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3165

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3166

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3167

SecurityFocus:

http://www.securityfocus.com/bid/69201

http://www.securityfocus.com/bid/69202

http://www.securityfocus.com/bid/69203